

**Några övningar inför lappskrivning nummer 3 på moment B, Diskret matematik för D2 och F, vt10.**

1. Betrakta den kropp med 8 element man får med hjälp av polynomet  $p(x) = x^3 + x + 1$ , dvs mängden

$$GF(8) = \{a_0 + a_1x + a_2x^2 \mid a_0, a_1, a_2 \in Z_2\},$$

och där man räknar som om  $p(x) = 0$  dvs som om  $x^3 = x + 1$ .

- (a) Beräkna  $(1 + x + x^2)(1 + x^2) + x + x^2$ .
  - (b) Bestäm inverserna till elementen  $1 + x$ ,  $x$  och  $x + x^2$ .
  - (c) Lös ekvationen  $(1 + x)z + x^2 = x$ .
  - (d) Bestäm tre olika generatorer till kroppens multiplikativa grupp.
2. Kunstruera kroppar, eller motivera varför de inte går att konstruera, om kropparna skall ha
- (a) 119 element.
  - (b) 120 element.
  - (c) 121 element.
3. En kropp  $F = GF(27)$  med 27 element konstrueras med hjälp av det i polynomringen  $Z_3[x]$  irreducibla polynomet  $p(x) = x^3 + 2x + 2$ .
- (a) Bestäm  $x^4$ ,  $x^5$  och  $x^6$ .
  - (b) Är  $p(x)$  ett primitivt polynom i ringen  $Z_3[x]$ .
  - (c) Bestäm en generator  $\alpha$  för kroppens multiplikativa grupp.
  - (d) Bestäm  $k$  sådant att  $\alpha^k = x^2 + 2$ .
  - (e) Har ekvationen  $z^2 + xz + 1 = 0$  några rötter i kroppen? Lös den i sådana fall.
4. Bestäm ett primitivt polynom  $p(x)$  av grad två i ringen  $Z_5[x]$ . Detta polynom kan på sedvanligt sätt användas för att definiera en kropp  $F$ .
- (a) Hur många element kommer denna kropp att ha?
  - (b) Bestäm tre olika generatorer för kroppens multiplikativa grupp.
  - (c) Bestäm samtliga lösningar i  $F$  till ekvationen  $z^3 = 1$ .
  - (d) Bestäm samtliga lösningar i  $F$  till ekvationen  $z^5 = 1$ .
5. Kan en kropp med 64 element ha en delkropp med
- (a) 2 element?
  - (b) 32 element?
6. Konstruera en kropp med 64 element som har en delkropp med 8 element. Kommer varje kropp med 64 element att ha en delkropp med 8 element?